UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/632,557	08/04/2000	Radia J. Perlman	SMY-009.02	1841

25181 7590 01/05/2005

FOLEY HOAG, LLP
PATENT GROUP, WORLD TRADE CENTER WEST
155 SEAPORT BLVD
BOSTON, MA 02110

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/632,557	PERLMAN ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-84* is/are pending in the application.

4a) Of the above claim(s) *65* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9,13,16-23,25-27,29,32,35-44,46,47,51,54-64,66,67,69-76 and 78-84* is/are rejected.

7)☐ Claim(s) *8,10-12,14,15,24,28,30,31,33-45,48-50,52,53,68 and 77* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment dated July 26, 2004 has been entered with the amendment on claims 1, 22, 41, 61, 66-68, 71, 76 and 84 and the deletion of claim 65.

2. Claims 1-84 are pending.

Response to Arguments

3. 35 USC 112 rejection on claim 84 is overcome by the amended claim.

4. Menezes et al. has been cited to address the amended claims, applicant's remarks regarding decryption with non-public key is acknowledged in Menezes.

5. Applicant argues that:

> "McManis does not prevent an interloper from inspecting the digest; the interloper need only use the sender's public key in order to decrypt it".

McManis discloses a naming service (Fig. 1, element 108) is a trusted service storing the public encryption keys that user and firewall computer both subscribe (col. 5, lines 55-58). So certainly, there are some levels of security when the service is subscribed with a trusted source.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-3, 16-17, 20-23, 25, 29, 35, 37, 39-44, 54-55, 59-65, 67-72, 76 and 81-82** are rejected under 35 U.S.C. 103(a) as being unpatentable over McManis, (5,850,449) in view of Menezes et al. (Handbook for Applied Cryptography).

a) **As to claims 1, 41, 71-72, 76, 81-82 and 84,** McManis discloses a system and method for sending packets of information between subscribers on a network and particularly a secure method of transmitting objects containing executable programs comprising an integrity check processor that selects one or more integrity functions, which reads on message digest, from a set of functions (Figure 6, element 604); manipulates m selected data bytes from each of one or more data packets, which reads on packet object (Figure 7), in accordance with the selected integrity check functions to produce one or more integrity checks that correspond to the one or more data packets (col. 5, lines 28-45); and an integrity block processor that encrypts the one or more integrity checks produced by the integrity check processor and produces an integrity block that is used to authenticate the data packets (col. 5, lines 46-65).

However, McManis does not disclose decyption using a non-public key.

Menezes discloses an authentication technique involves the use of a secret key to generate a cryptographic checksum or MAC (message authentication code). In this technique, two communicating parties share a common secret key, therefore the recipient performs the decryption only with a non-public key (pages 323-327)

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of a secret key to generate a MAC, as Menezes teaches, in the system of McManis so as to provide the ease of computation (page 325).

b) **As to claims 2-3, 44 and 63-64,** McManis discloses the system wherein the integrity check processor includes in the integrity check an indication of which integrity function to select and the indication is a function identifier (col. 5, lines 29-30).

c) **As to claims 16-17, 35, 54-55 and 69-70,** McManis discloses the data authentication system wherein the integrity check processor produces digital signatures for one or more of the data packets and includes the digital signatures in the respective data packets (col. 5, lines 59-61).

d) **As to claims 20-21, 39-40, 59-60 and 67-68,** McManis discloses the system wherein the integrity block processor encrypts into the integrity block executable code that performs the selected integrity check function (Figure 6) and signs the executable code with a digital signature (col. 4, lines 48-52, Figure 7).

e) **As to claims 22 and 25,** McManis discloses a communications network comprising one or more sending stations for sending data packets (Figure 1, element 102); one or more recipient stations for receiving the data packets sent by the sending stations (Figure 1, element 103); an authentication system (Figure 1, element 105) that

includes an integrity block processor for selecting one or more integrity functions from a set of integrity functions (see addressed claim 1), manipulating one or more selected data bytes from a given data packet in accordance with the one or more selected integrity check functions to produce the corresponding integrity checks (see addressed claim 1) and encrypting the one or more integrity checks that are associated with one or more data packets to produce an integrity block and including the integrity block in a transmission to the recipient stations (see addressed claim 1) and authentication means for decrypting a received integrity block to reproduce the one or more integrity checks and using information contained in the reproduced integrity checks to select one or more integrity check functions and one or more data bytes to use to determine if data in the associated one or more data packets have been altered (col. 6, lines 25-54).

f) **As to claim 23,** McManis discloses the communications network wherein the authentication means selects the one or more integrity check functions for use in authenticating the data packets based on identifying information in the associated integrity check (col. 6, lines 35-41).

g) **As to claim 29,** McManis discloses the communications network wherein the integrity block processor encrypts into an integrity block the information that identifies the integrity check function (col. 5, lines 28-58).

h) **As to claim 37,** McManis discloses the system wherein the authentication means encodes selected bytes from a given data packet to produce the associated integrity check (col. 5, lines 26-28).

i) **As to claims 42 and 43,** McManis discloses the method further including the steps of decrypting a received integrity block to reproduce the integrity check (Figure 6, step 618); selecting one or more integrity check functions from the set of functions and using the reproduced integrity check and the selected integrity check functions to determine if the first data packet is authentic (Figure 6, step 620).

Part of claim 43 is also addressed in claim 1.

j) **As to claims 61-62,** McManis discloses a data authentication system comprising an integrity block processor that receives a plurality of data packets and an associated integrity block, the integrity block processor manipulating the integrity block to produce a plurality of integrity checks that correspond to the data packets and an integrity check processor that uses the integrity checks, the integrity check functions selected from a set of functions and selected data bytes from the data packets to determine if any of the data packets have been altered (col. 6, lines 25-54).

8. **Claims 4-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over McManis, (5,850,449) in view of Menezes et al. (Handbook for Applied Cryptography), and further in view of Koopman, (Re. 36,752).

McManis discloses a secure system and method for sending packets of information between subscribers on a network, however he fails to disclose a system wherein the indication is an offset value for a pseudorandom sequence.

Koopman discloses a system wherein the indication is an offset value for a pseudorandom sequence that is generated using a seed value known by the sender and the intended recipient (col. 5, lines 40-43; col. 11, lines 15-17).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of offset value for a pseudorandom sequence as integrity indication and the use of seed value to generate pseudorandom sequence, as Koopman teaches, in the system of McManis and Stallings so as to provide another particular way to perform integrity check on information sent over a communications network.

9. **Claims 9, 18, 27, 36-37, 46-47, 56-57, 66 and 78-80** are rejected under 35 U.S.C. 103(a) as being unpatentable over McManis, (5,850,449) in view of Menezes et al. (Handbook for Applied Cryptography), and further in view of Augustine, (5,440,633).

a) **As to claims 9, 27, 46-47, 66 and 78,** McManis discloses a secure system and method for sending packets of information between subscribers on a network wherein the integrity block processor encrypts the integrity checks in accordance with a private/public key (col. 5, lines 46-58), not with a shared secret key.

Augustine discloses the integrity checks are encrypted in accordance with a shared secret key that is shared by intended recipients of the data packets (Figure 3, element 29; col. 5, lines 49-54).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of shared secret key, as Augustine teaches, in the system of McManis and Stallings so as to provide another particular encryption key to secure information sent over a communications network.

b) **As to claims 18, 36-37, 56-57 and 79-80,** McManis discloses a secure system and method for sending packets of information between subscribers on a network, however he fails to disclose the selected integrity check function concatenates the selected data bytes from a given data packet to produce the associated integrity check.

Augustine discloses the selected integrity check function concatenates the selected data bytes from a given data packet to produce the associated integrity check (col. 4, lines 36-38; col. 5, lines 14-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of concatenating the selected data bytes from a given data packet to form the integrity check, as Augustine teaches, in the system of McManis and Stallings, so as to provide another particular way perform integrity check on information sent over a communications network.

10. Claims 13, 19, 32, 38, 51, 58, 75 and 83 are rejected under 35 U.S.C. 103(a) as being unpatentable over McManis, (5,850,449) in view of Menezes et al. (Handbook for Applied Cryptography), and further in view of Rivest.

a) **As to claims 13, 32 and 51,** McManis discloses a secure system and method for sending packets of information between subscribers on a network, however he fails to disclose the sequence number associated with the data packet is not included in the integrity check.

Rivest discloses one or more sequence numbers that are associated with the data packets are included in the integrity checks (page 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sequence number, as Rivest teaches, in the system of McManis and Stallings so as to correctly order the received packets when reassembling the information.

b) **As to claims 19, 38, 58, 75 and 83,** McManis discloses a secure system and method for sending packets of information between subscribers on a network, however he fails to disclose the system further including a chaff processor.

Rivest discloses chaffing process for producing for transmission extraneous packets that are associated with and do not pass one or more of the integrity checks, the chaff processor including the extraneous packets in a transmission that includes the data packets (page 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of chaffing process, as Rivest teaches, in the system of McManis and Stallings so as to better secure the confidentiality of information sent over a communications network.

11. **Claims 26, 73-74** are rejected under 35 U.S.C. 103(a) as being unpatentable over McManis, (5,850,449) in view of Menezes et al. (Handbook for Applied Cryptography), and further in view of Kingdon, (5,349,642).

McManis discloses a secure system and method for sending packets of information between subscribers on a network, however he fails to disclose the communications network wherein the integrity block processor is included in each of the one or more sending stations and the authentication means is included in each of the one or more recipient stations.

Kingdon discloses the system wherein the integrity block processor is included in each of the one or more sending stations and the authentication means is included in each of the one or more recipient stations (Figure 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the integrity block processor in each sending stations and having the authentication means in each of the recipient stations, as Kingdon teaches, in the system of McManis and Stallings so as to conveniently verify the integrity of the information sent over a communications network.

Allowable Subject Matter

12. **Claims 8, 10-12, 14-15, 24, 28, 30-31, 33-34, 45, 48-50, 52-53, 68 and 77** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
12/29/04

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER